16 V 88

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 4 : H04L 9/00

A1

(11) International Publication Number: WO 88/ 01119

(43) International Publication Date: 11 February 1988 (11.02.88)

(21) International Application Number: PCT/GB87/00557

(22) International Filing Date: 6 August 1987 (06.08.87)

(31) Priority Application Number: 8619453

(32) Priority Date: 8 August 1986 (08.08.86)

(33) Priority Country: GB

(71) Applicant *(for all designated States except US):* BRITISH BROADCASTING CORPORATION [GB/GB]; Broadcasting House, London W1A 1AA (GB).

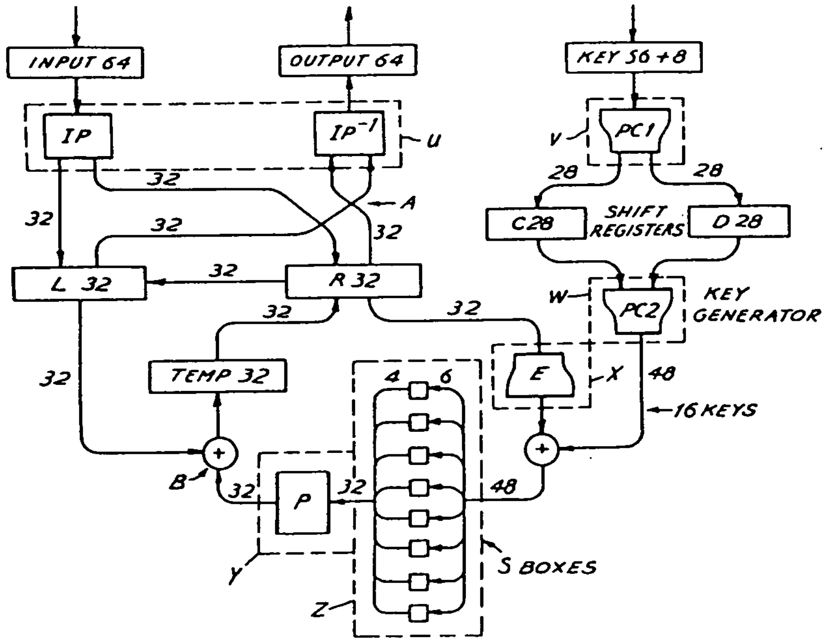
(72) Inventors; and
(75) Inventors/Applicants *(for US only)* : CHAMBERS, John, Philip [GB/GB]; 24 Green Lane, Tadworth, Surrey KT20 6TL (GB). WRIGHT, Derek, Thomas [GB/GB]; 30 Lashmere, Copthorne, West Sussex RE10 3RT (GB).

(74) Agent: ABNETT, Richard, Charles; Reddie & Grose, 16 Theobalds Road, London WC1X 8PL (GB).

(81) Designated States: AT (European patent), BE (European patent), CH (European patent), DE (European patent), FR (European patent), GB (European patent), IT (European patent), JP, LU (European patent), NL (European patent), SE (European patent), US.

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: DATA ENCIPHERMENT



(57) Abstract

Data encipherment and decipherment is achieved by converting blocks of input bits into blocks of output bits. The input bits are subjected to the operation of an algorithm, such as in accordance with the DES standard, involving a plurality of bit-permutation and/or substitution operations selected under the control of a key of substantial length. In the invention the operations available for selection by the key are changed in response to operation-control data received from an external source such as one involving the use of teletext or videotext, or using card or bar code readers, or direct keyboard input.

DATA ENCIPHERMENT

BACKGROUND OF THE INVENTION

This invention relates to a data encipherment apparatus and method which converts a block of input bits into a block of output bits under the control of a key of substantial length.

Several data encryption algorithms have been defined where the input data is converted into output data by passing it through a succession of bit-permutation operations (re-arranging the order of the bits in the data word) and substitution tables (groups of bits are used to address tables which produce new bit patterns). Typical algorithms have input and output words of 64 bits and are controlled by a key of up to 64 bits in length. The exact process of the conversion depends in each case not only on a key variable which acts upon the data path, but also upon the definitions of the bit permutations and substitution tables around which the algorithm is constructed.

One example of such an encryption method is known as DES and published by U.S. National Bureau of Standards, "Data Encryption Standard", Federal Information Processing Standards Publication 46 (January 15, 1977). This specification assumes a knowledge of this standard.

The DES standard defines an algorithm based upon five bit-permutation operations and eight substitution tables. The bit permutation tables are themselves each defined by a table which lists, for each output bit, the bit number of the corresponding input bit. An output bit cannot be fed from more than one input bit but it is possible for two or more output bits to be fed from the same input bit (this is known as an expanded permutation) or for some input bits to not be used at all (a permuted choice).

In a software realisation of the algorithm the substitution tables and the tables defining the bit permutations would be stored as data constants in read only memory.

Other examples of encipherment algorithms using bit permutations and/or substitutions are to be found in our British Patent Applications Nos. 8607961 and 8610733 (International Patent

Applications PCT/GB87/00216 and PCT/GB87/00266).

SUMMARY OF THE INVENTION

According to this invention we provide a data cipherment method and apparatus for converting a block of input bits into a block of output bits, in which data is subjected to the operation of an algorithm defining a plurality of bit-permutation and/or substitution operations selected under the control of a key of substantial length, in which the operations available for selection by the key can be changed in response to operation-control data obtained from an external source.

In this specification the term cipherment is used to cover both encipherment and decipherment.

Thus for example with the DES algorithm instead of storing the substitution and bit-permutation tables in read-only memory they are stored in read/write memory so that they can be loaded with data obtained from an external source. The source may involve the use of transmission techniques such as teletext or videotex (Prestel) or input techniques such as card readers, bar code readers, or direct keyboard input.

This enables the effect of the algorithm to be changed in a more drastic way than by changing the key variable alone. The changed algorithm is then no longer the defined DES algorithm but one of very many possible variants of it. The data loaded into the tables must conform to various restrictions imposed for the particular type of algorithm being modified.

BRIEF DESCRIPTION OF THE DRAWING

The invention will be described in more detail with reference to the DES algorithm as illustrated by the accompanying drawing in which the sole figure is a flow chart illustrating the logical structure of the DES algorithm.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

As the DES algorithm is itself known detailed description of the drawing is not deemed necessary, and reference should be made to the DES standard noted above. (This is reprinted with additional comment in "Cipher Systems" by H. Beker and F. Piper published by Northwood Publications 1982 ISBN 7198 2611 X). The figure in the drawing is taken from page 55 of "Security for Computer Networks" by D.W. Davies and W.L. Price published by John Wiley and Sons, ISBN 0 471 90063 X. Reference should be made to that book for a detailed description of the figure. The algorithm comprises a succession of five bit-permutation operations PC1, PC2, IP, IP^{-1} and E, in which the order of the bits in the data word is re-arranged, and eight substitution tables in the S boxes in which groups of bits are applied as inputs to look-up tables which produce new bit patterns. PC1 and PC2 are permuted choice and E is an expanded permutation. The number of bits being processed at various points is indicated on the figure.

It is seen in the drawing that some of the operations are outlined by dashed boxes U to Z. These boxes define areas capable of external re-definition. These areas provide changeable data as follows:

Table of Changeable Data

Dashed Box	Operations	Words	x	Bits	Total
U	IP and IP^{-1}	64	x	6	384
V	PC1	56	x	6	336
W	PC2	48	x	6	288
X	E	48	x	5	240
Y	P	32	x	5	160
Z	S boxes	8 x 64	x	4	2048
				TOTAL:	3456

Thus for the DES algorithm the total data content of all the bit-permutation and substitution tables approaches 3500 bits. This gives greater freedom for change than the existing 56-bit key variable alone.

In the absence of an external source of data for loading the tables in read/write memory, a suitable set of default values could be transferred to the read/write memory from an area of read only memory. Another possibility is for partial modification of the table contents starting with initial values obtained from read only memory.

The data for modifying the table contents could be carried over the chosen transport channel enciphered by a further algorithm and key at a higher level of security. It could alternatively be carried by mechanical or physical methods (e.g. punched cards, magnetic cards, printed bar codes, typewritten numbers) and distributed by post or courier. Also a point-to-point electrical connection could be used (landline or telephone).

In a hardware realisation of the algorithm it would be considerably more difficult to change the bit permutations under the control of external data but there is still the possiblity of modifying the contents of the substitution tables.

Similar principles to those described for use with the DES algorithm could be used to vary the algorithms the subject of our British Patent Applications Nos. 8607961 and 8610733 (International Patent Applications PCT/GB87/00216 and PCT/GB87/00266). In the first of these the algorithm consists of a series of bit permutations dependent upon a keyword, and in the second it consists of a repeated permutation and substitution sequence with the initial substitution pattern dependent upon a control word.

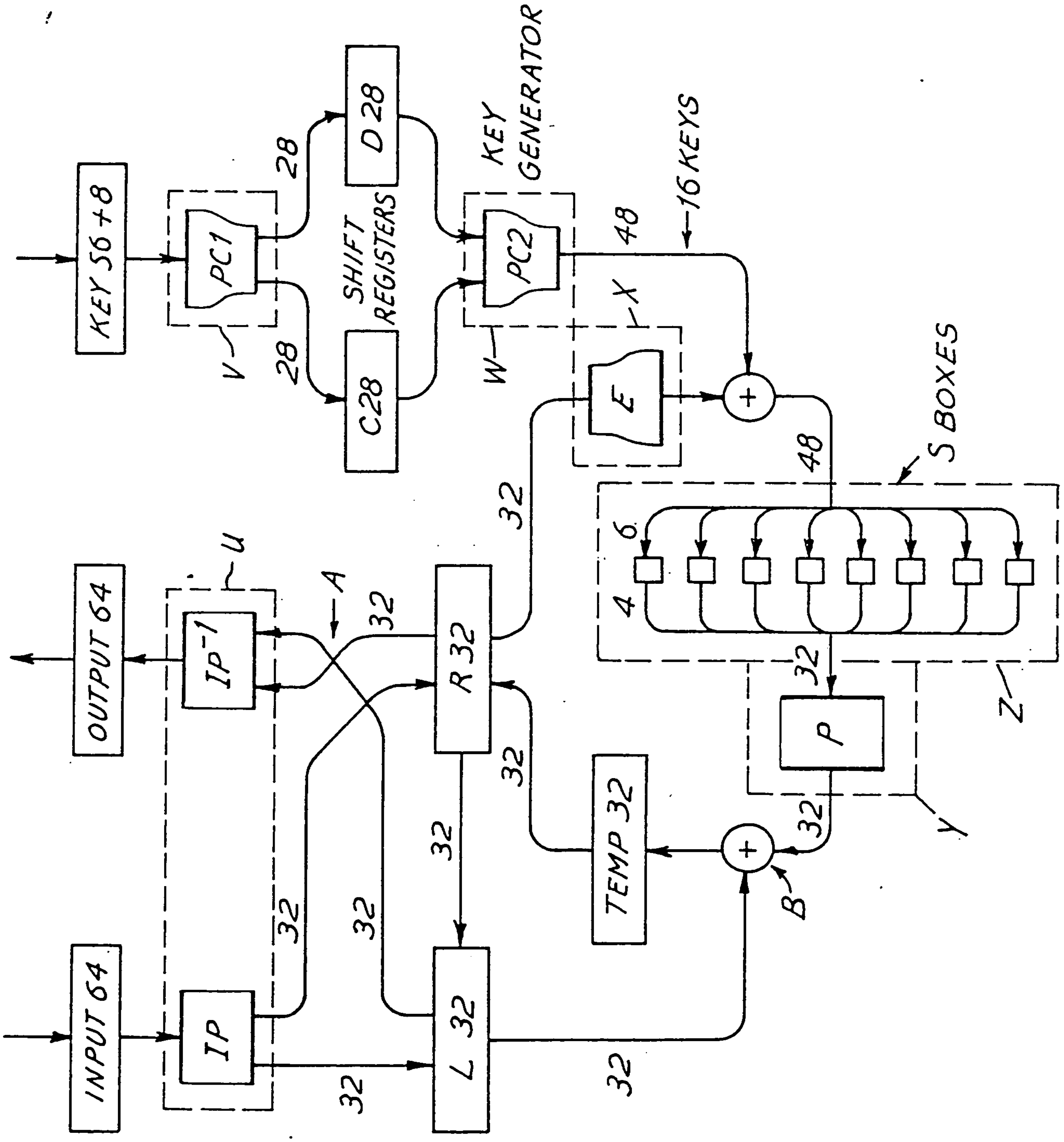
CLAIMS

1. A method of data cipherment in which blocks of input bits are converted into blocks of output bits, comprising subjecting the input bits to the operation of an algorithm defining a plurality of bit-permutation and/or substitution operations selected under the control of a key of substantial length, and changing the operations available for selection by the key in response to operation-control data received from an external source.

2. Data cipherment apparatus for converting blocks of input bits into blocks of output bits, comprising storage means for storing bit-permutation and/or substitution tables defined by an algorithm, data conversion means for subjecting input bits to a plurality of bit-permutation and/or substitution operations defined by the tables in the storage means as selected under the control of a key of substantial length to provide the output bits; and means for changing the stored tables in response to operation-control data received from an external source.

3. Apparatus according to claim 2, in which the algorithm is based on the DES algorithm.

1/1


KEY 56+8
PC1
V
28
28
SHIFT REGISTERS
D 28
C28
KEY GENERATOR
PC2
W
48
16 KEYS
X
E
32
S BOXES
48
6
4
32
P
Z
Y
32
B
TEMP 32
32
R 32
32
A
32
32
32
L 32
32
32
INPUT 64
IP
IP^{-1}
U
OUTPUT 64

INTERNATIONAL SEARCH REPORT

International Application No PCT/GB 87/00557

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) [6]

According to International Patent Classification (IPC) or to both National Classification and IPC

IPC^4: H 04 L 9/00

II. FIELDS SEARCHED

Minimum Documentation Searched [7]

Classification System	Classification Symbols
IPC^4	H 04 L

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched [8]

III. DOCUMENTS CONSIDERED TO BE RELEVANT [9]

Category [*]	Citation of Document, [11] with indication, where appropriate, of the relevant passages [12]	Relevant to Claim No. [13]
Y	Proceedings of the IEEE, volume 67, no. 3, March 1979, IEEE, (New York, US), W. Diffie et al.: "Privacy and authentication: an introduction to cryptography", pages 397-427 see page 409, left-hand column, lines 18-42; figures 11,12	1
A		3
	--	
Y	FR, A, 2486680 (T.R.T.) 15 January 1982 see page 1, line 23 - last line; page 2, line 21 - page 3, line 28; figure 1	1
	--	
A	US, A, 4275265 (DAVIDA) 23 June 1981 see column 6, lines 22-58	1
	--	
P,X	EP, A1, 0202989 (THOMSON-CSF) 26 November 1986 see column 2, lines 1-11; column 3, line 15 - column 4, line 18; column 5, lines 34-48; column 6, lines 42-55	1,2
	--------	

* Special categories of cited documents: [10]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search 4th November 1987	Date of Mailing of this International Search Report - 4 DEC 1987
International Searching Authority EUROPEAN PATENT OFFICE	Signature of Authorized Officer M. VAN MOL

ANNEX TO THE INTERNATIONAL SEARCH REPORT ON

INTERNATIONAL APPLICATION NO. PCT/GB 87/00557 (SA 18183)

This Annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report. The members are as contained in the European Patent Office EDP file on 16/11/87

The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR-A- 2486680	15/01/82	None	
US-A- 4275265	23/06/81	None	
EP-A- 0202989	26/11/86	FR-A- 2582174 JP-A- 61261773	21/11/86 19/11/86

For more details about this annex :
see Official Journal of the European Patent Office, No. 12/82